PCT/JP98/01837
22.04.98

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

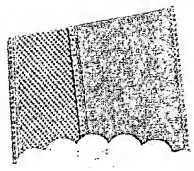
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

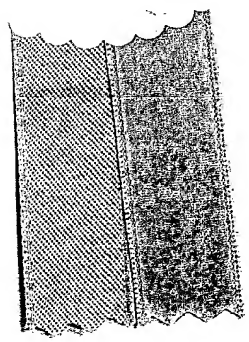
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９７年 ４月２４日

出 願 番 号
Application Number: 平成 ９年特許願第１０６９９５号

出 願 人
Applicant (s): 松下電器産業株式会社





１９９８年 ６月 ５日

特 許 庁 長 官
Commissioner,
Patent Office

荒井寿光

出証番号 出証特平１０－３０４２５１２

【書類名】　特許願

【整理番号】　2054091207

【提出日】　平成 9年 4月24日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 13/00

【発明の名称】　データ転送方法

【請求項の数】　13

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　西村　拓也

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　飯塚　裕之

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　山田　正純

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100078204

【弁理士】

【氏名又は名称】　滝本　智之

【選任した代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9702380

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ転送方法

【特許請求の範囲】

【請求項１】　バス上の任意の機器が同期データを受信する同期通信と、非同期データを受信する機器が特定される非同期通信とが混在するバスシステムにおいて、前記同期データは実データ部を含む場合があり、前記実データ部の暗号化状況を示す暗号識別情報が前記実データ部以外の前記同期データ中に含まれており、前記同期データを受信した受信装置は、前記実データ部が暗号化されていることを前記暗号識別情報が示している場合には前記同期データを送信している送信装置に対して前記非同期通信を用いて前記実データ部の復号化情報を要求し、前記要求を受けた前記送信装置は前記非同期通信を用いて前記受信装置に対して前記実データの復号化情報を暗号化して送信し、前記受信装置は前記暗号化された復号化情報から前記復号化情報を取り出し、前記復号化情報を用いて暗号化された実データ部を復号することを特徴とするデータ転送方法。

【請求項２】　同期データを受信した受信装置が実データ部が暗号化されていることを検出してから復号化情報を取得するまでの一連の手順には複数の種類が存在し、前記受信装置は復号化情報の要求に先立って送信装置が実行可能な手順の種類を前記送信装置に問い合わせ、前記受信装置は自身と前記送信装置との双方が実行可能な前記手順の中から実行する手順を選択し、前記受信装置は選択した手順に基づいて前記復号化情報を取得することを特徴とする請求項１記載のデータ転送方法。

【請求項３】　選択された手順に基づいて送信装置と受信装置との間で授受される非同期データには、実行中の前記手順の種類をあらわす手順識別子が含まれることを特徴とする請求項２記載のデータ転送方法。

【請求項４】　受信装置は、復号化情報の要求を行う前に、送信装置が正規の送信装置であることを確認することを特徴とする請求項１、２または３記載のデータ転送方法。

【請求項５】　送信装置は復号化情報の要求を受けた後、受信装置が正規の受信装置であることを確認してから実データの復号化情報を暗号化して送信するこ

とを特徴とする請求項１、２または３記載のデータ転送方法。

【請求項６】　送信装置と受信装置とが互いに、相手が正規の受信装置または正規の送信装置であることを確認してから前記受信装置が復号化情報の要求を行うことを特徴とする請求項１、２または３記載のデータ転送方法。

【請求項７】　受信装置が復号化情報を要求する前に、前記受信装置から送信装置に対して前記送信装置が共通鍵を作成するのに少なくとも必要な情報の送信と、前記送信装置から前記受信装置に対して前記受信装置が前記共通鍵を作成するのに少なくとも必要な情報の送信とが行われ、前記送信装置は前記共通鍵を用いて前記復号化情報を暗号化して送信し、前記受信装置は前記共通鍵を用いて前記復号化情報を取り出すことを特徴とする請求項１ないし６のいずれかに記載のデータ転送方法。

【請求項８】　暗号化は実データ部に対してのみ行うことを特徴とする請求項１、２または３記載のデータ転送方法。

【請求項９】　送信装置は内部に実データの信号源を有し、前記送信装置は前記信号源から出力された固定長単位の前記実データ毎に暗号化の有無を決定し、暗号化された前記実データと暗号化されていない前記実データとを互いに異なる同期通信の出力単位内に配置してバスシステムへ出力することを特徴とする請求項１、２または３記載のデータ転送方法。

【請求項１０】　暗号化された実データと、暗号化されない実データとの比率を受信装置が送信装置に対して非同期通信を用いて指定し、前記送信装置は前記指定に従って暗号化の有無の比率を変更することを特徴とする請求項９記載のデータ転送方法。

【請求項１１】　送信装置は内部に実データの信号源を有し、前記送信装置は前記信号源から出力された固定長単位の前記実データについて、前記固定長単位の中での暗号化を行う割合を決定し、前記実データを同期通信の出力単位内に配置してバスシステムへ出力することを特徴とする請求項１、２または３記載のデータ転送方法。

【請求項１２】　受信装置は送信装置に対して、暗号化を行う割合の指定を非同期通信を用いて行い、前記送信装置は前記指定に従って暗号化する割合を変更

することを特徴とする請求項１１記載のデータ転送方法。

【請求項１３】　送信装置が同期データを送信する際に、少なくとも復号化情報を要求されるまでの間は前記同期データに実データ部を含めずに送信し、少なくとも前記復号化情報の要求を受け取った後に前記実データ部を含んだ前記同期データの送信を開始することを特徴とする請求項１、２または３記載のデータ転送方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ディジタルデータを送受信する機器間のデータ転送方法に関するものである。

【０００２】

【従来の技術】

従来のデータ転送方式には、ＩＥＥＥ１３９４規格（IEEE:THE INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, INC）を用いたデータ転送方法がある。（参考文献：IEEE1394 High Performance Serial Bus）ＩＥＥＥ１３９４規格におけるデータ転送には、映像信号や音声信号等の同期データの転送に適したアイソクロノス通信と、制御信号等の非同期データの転送に適したエイシンクロナス通信とがあり、両通信はＩＥＥＥ１３９４バス上で混在することが可能である。アイソクロノス通信はいわゆる放送型の通信であり、ＩＥＥＥ１３９４バス上のある装置が出力するアイソクロノスパケットは、同バス上の全ての装置が受信することができる。これに対してエイシンクロナス通信は１対１の通信と放送型通信の両方があり、バス上のある装置が出力するエイシンクロナスパケットにはそのパケットを受信すべき装置をあらわす識別子が含まれており、その識別子が特定の装置をあらわす時にはその識別子で指定された装置が当該エイシンクロナスパケットを受信し、識別子がブロードキャストをあらわす時には同バス上の全ての装置が当該エイシンクロナスパケットを受信する。

【０００３】

また、ＩＥＥＥ１３９４規格を用いてディジタル音声信号やディジタル映像信

号等を転送したり、ＩＥＥＥ１３９４バス上につながれた機器間でデータ伝送経路の接続管理を行うための規格として、ＩＥＣ（IEC:International Electronical Commission 国際電気標準会議）においてＩＥＣ１８８３規格（以下、ＡＶプロトコルと称する）が検討されている。ＡＶプロトコルにおいては、映像音声データはアイソクロノスパケット内に配置されて転送される。また、アイソクロノスパケットはＣＩＰヘッダ（CIP:Common Isochronous Packet）を含む。ＣＩＰヘッダ内には映像音声データの種類を示す識別情報や、アイソクロノスパケットを送信している送信装置の装置番号等の情報が含まれている。

【０００４】

図５は、ＡＶプロトコルにて使用されるアイソクロノスパケットのフォーマットをあらわす図である。アイソクロノスパケットはアイソクロノスパケットヘッダ９００、ヘッダＣＲＣ９０１、アイソクロノスペイロード９０２、データＣＲＣ９０３からなる。アイソクロノスパケットヘッダ９００にはタグ９０７が含まれる。タグ９０７は、その値が１である時にはそのアイソクロノスパケットがＡＶプロトコルに準拠したアイソクロノスパケットであることを示す。タグ９０７の値が１であるとき、即ち、そのアイソクロノスパケットがＡＶプロトコル準拠のアイソクロノスパケットである時には、アイソクロノスペイロード９０２の先頭にＣＩＰヘッダ９０４が含まれる。ＣＩＰヘッダ９０４の中には、当該アイソクロノスパケットを出力している出力装置の識別子であるソースＩＤ９０６が含まれる。また、ＣＩＰヘッダ９０４にはアイソクロノスペイロード９０２に含まれる実データ９０５がどの様な種類のデータであるかをあらわすＦＭＴ９０８やＦＤＦ９０９が含まれる。映像や音声の信号は実データ９０５に含まれるが、実データ９０５はアイソクロノスペイロード９０２にかならず含まれるとは限らず、パケットによっては実データ９０５を含まずにＣＩＰヘッダ９０４のみを含むアイソクロノスペイロード９０２も有り得る。

【０００５】

また、ＡＶプロトコル上で機器制御を行うためのコマンド群として、ＡＶ／Ｃコマンドセットがある。例えば、「1394 TRADE ASSOCIATION Specification for AV/C Digital Interface Command Set Version 1.0」 September 13, 1996に詳

しい。これらのコマンドとその応答はエイシンクロナス通信を用いて転送される。

【０００６】

【発明が解決しようとする課題】

上記従来のデータ転送方法において、著作権保護のためにアイソクロノス通信のアイソクロノスペイロード９０２を暗号化して送信しようとすると、暗号化されたアイソクロノスペイロード９０２の転送に対応していない従来の機器との互換性を保つことができない。すなわち、従来の機器はアイソクロノスペイロード９０２の先頭にＣＩＰヘッダ９０４が正常に配置されて送信されてくることを前提に作られており、アイソクロノスペイロード９０２が暗号化されてＣＩＰヘッダ９０４が正常に読み出せない場合には、そのアイソクロノスパケットはＡＶプロトコルを満たさないものとなるとともに、暗号化されたアイソクロノスパケットを受信した受信装置は正常に動作することができなくなる。すなわち実データ９０５に含まれる映像音声データがどのような種類のデータであるかを判別することが不可能であるとともに、当該アイソクロノスパケットを出力している装置を特定することが不可能になるので送信装置に対する各種の問い合わせ等の通信を行うことができなくなり、受信動作を正常に行うことが不可能となってしまうという課題があった。

【０００７】

また、上記従来のデータ転送方法において、送信装置が出力するアイソクロノスパケットを受信装置が継続して受信している最中にアイソクロノスパケットの暗号化が始まるような場合、従来の機器においては暗号化が始まった途端にＣＩＰヘッダ９０４を正常に読み出すことができなくなり、正常な受信が行えなくなるという課題があった。

【０００８】

また、送信装置が、著作権で保護されている映像音声情報等を暗号化して送信し、正規に認められた受信装置が暗号化された映像音声データ等を復号化するためには、送信装置から正規の受信装置に対して復号のための鍵情報を付与する必要があるが、上記従来のデータ転送方法においては送信装置が受信装置を特定す

るには非常に煩雑な手順を実行せねばならない。すなわちアイソクロノスパケットには、送信を行っている装置の識別子であるソースＩＤ９０６は含まれるが、どの装置が当該アイソクロノスパケットを受信するべきであるかをあらわす情報は含まれておらず、送信装置には、どの装置が当該アイソクロノスパケットの受信を行っているかを直接的に調べることはできない。そこで、送信装置において、ＩＥＥＥ１３９４バス上に接続されている機器のうちのどの機器が受信を行っており、どの機器が受信を行っていないかを調べるにはバス上の全ての機器に対して受信状態の問い合わせを行わねばならず、非常に煩雑であるという課題があった。

【０００９】

本発明は上記従来の問題点を解決するもので、暗号化した映像音声情報をアイソクロノス通信で送信する場合にも従来の通信規格を満足し、かつ従来の受信装置が暗号化された映像音声データを含むアイソクロノスパケットを受信しても誤動作することのないデータ転送方法を実現することを目的とする。

【００１０】

また、本発明は、送信装置が正規の受信装置に復号のための鍵情報を付与する際の手順を極めて簡素なものとすることが可能なデータ転送方法を実現することを目的とする。

【００１１】

【課題を解決するための手段】

上記従来のデータ転送方法の問題点を解決するために、本発明のデータ転送方法は、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行い、データ転送を行う。

【００１２】

また、本発明のデータ転送方法は、同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データと一緒に送信され、実データ部が暗号化されていることを検出した受信装置が送信装置に対して復号化情報を要求し、受信装置は送信装置から受け取った復号化情報を使用して実データ部の復号化を行うことによ

ってデータ転送が行われる。

【0013】

【発明の実施の形態】

本発明は、バス上の任意の機器が同期データを受信する同期通信と、非同期データを受信する機器が特定される非同期通信とが混在するバスシステムにおいて、前記同期データは実データ部を含む場合があり、前記実データ部の暗号化状況を示す暗号識別情報が前記実データ部以外の前記同期データ中に含まれており、前記同期データを受信した受信装置は、前記実データ部が暗号化されていることを前記暗号識別情報が示している場合には前記同期データを送信している送信装置に対して前記非同期通信を用いて前記実データ部の復号化情報を要求し、前記要求を受けた前記送信装置は前記非同期通信を用いて前記受信装置に対して前記実データの復号化情報を暗号化して送信し、前記受信装置は前記暗号化された復号化情報から前記復号化情報を取り出し、前記復号化情報を用いて暗号化された実データ部を復号する。

【0014】

これにより、以下のような作用を有する。

まず、同期データを受信した受信装置が同期データ内に含まれる暗号識別情報を調べ、実データ部が暗号化されていることを検出すると送信装置に対して実データ部を復号するための復号化情報を要求する。この要求は非同期通信を用いて行われ、この要求を受け取った送信装置においては、非同期通信のパケットヘッダを調べることにより要求を出した機器すなわち受信装置が特定される。ここで特定された受信装置に対して送信装置が復号化情報を付与することにより、送信装置が受信装置に復号のための鍵情報を付与する際の手順が極めて簡素なデータ転送方法を実現できる。

【0015】

また、同期データの暗号化は実データ部のみに対して行われ、同期データには実データ部の暗号化状況を示す暗号識別情報が含まれる。これにより、ＣＩＰヘッダは暗号化されずにそのまま転送されるので従来の装置がこれらの暗号化された同期データを受信しても誤動作することはない。すなわち、従来のデータ転送

方法との互換性を保ちつつ、かつ従来の受信装置が同期データを受信しても誤動作する可能性の無いデータ転送方法を実現できる。

【００１６】

また、送信装置の送信している同期データを受信装置が継続的に受信している最中に同期データの暗号化が始まったとしても、ＣＩＰヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できる。

【００１７】

以下、本発明の実施の形態について、図面を参照しながら説明する。

図１は、本発明の実施の形態において転送されるアイソクロノスパケットのペイロード部の形式を表した図である。本実施の形態は、ＭＰＥＧのＴＳＰ（トランスポートパケット）の伝送を例とする。暗号化情報（ＥＮＣ）９１０は実データ９０５が暗号化されているか否かを示す。

【００１８】

図２は、本実施の形態における送信装置と受信装置の関係をあらわすブロック図である。図２において、送信装置１１０と受信装置１２８とは１３９４バス１１１を通じてつながれている。信号源１００は、１３９４バス１１１上に送信しようとする１８８バイト単位のＭＰＥＧのＴＳＰ（図示せず）を暗号化手段１０１に対して出力する。すなわち本実施の形態では、信号源１００は１８８バイトの固定長のデータを出力する。暗号化手段１０１は、鍵生成手段１０６から与えられる暗号鍵１０９を用いて信号源１００から入力したＴＳＰを暗号化して出力する。本実施の形態では暗号鍵１０９が復号化情報に相当する。鍵生成手段１０６からの出力命令１０５は、暗号化手段１０１に対する命令であり、通常出力、暗号化出力、空出力の３種類の命令がある。出力命令１０５を入力した暗号化手段１０１は、その命令の内容が通常出力である場合には、信号源１００から入力したＴＳＰをそのまま出力し、暗号化情報９１０には値０を出力する。また出力命令１０５の内容が暗号化出力である場合には、ＴＳＰを、鍵生成手段１０６から受け取った暗号鍵１０９で暗号化して出力し、暗号化情報９１０には値１を出力する。また出力命令１０５の内容が空出力である場合には、信号源１００から

ＴＳＰを受け取るたびに空信号（図示せず）を出力するとともに、暗号化情報９１０には値１を出力する。

【００１９】

ソースパケット化手段１０２は、暗号化手段１０１から入力した１８８バイトのＴＳＰに４バイトのソースパケットヘッダを付加して１９２バイトのソースパケットを出力する。ＣＩＰブロック化手段１０３は、ソースパケット化手段１０２から受け取ったソースパケットにＣＩＰヘッダ９５４を付加して出力する。その際にＣＩＰブロック化手段１０３は、暗号化手段１０１から入力した暗号化情報９１０をＣＩＰヘッダ９５４内に配置する。アイソクロノスパケット化手段１０７はＣＩＰブロック化手段１０３から入力したパケットにアイソクロノスパケットヘッダ９００、ヘッダＣＲＣ９０１およびデータＣＲＣ９０３を付加して出力する。このとき、アイソクロノスペイロード９５２の内容がＡＶプロトコルに準拠したデータであるので、タグ９０７の値は１とする。鍵生成手段１０６は、受信装置１２８との間のエイシンクロナス通信のやり取りにより暗号鍵１０９を受信装置１２８に送信するとともに暗号化手段１０１に対しても出力する。

【００２０】

１３９４パケット入出力手段１０８は１３９４バス１１１と送信装置１１０との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、アイソクロノスパケット化手段１０７の出力するアイソクロノスパケットおよび鍵生成手段１０６の出力するエイシンクロナスパケットを１３９４バス１１１上に出力するとともに、１３９４バス１１１から受信したエイシンクロナスパケットを鍵生成手段１０６へと出力する。

【００２１】

１３９４パケット入出力手段１２７は、１３９４バス１１１と受信装置１２８との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、１３９４バス１１１から受信したアイソクロノスパケットをペイロード抽出手段１２３に対して出力し、１３９４バス１１１から受信したエイシンクロナスパケットを鍵生成手段１２５に対して出力する。また、鍵生成手段１２５の出力するエイシンクロナスパケットを１３９４バス１１１に対して出力す

る。

【００２２】

ペイロード抽出手段１２３は、１３９４バス１１１から受信したアイソクロノスパケットを１３９４パケット入出力手段１２７から入力し、アイソクロノスパケットのタグ９０７の値が１である場合にはアイソクロノスペイロード９５２の中身がＡＶプロトコル準拠のデータであることを知り、アイソクロノスペイロード９５２を実データ抽出手段１２２に対して出力する。実データ抽出手段１２２は、受け取ったアイソクロノスペイロード９５２に実データ９０５が含まれる場合には、アイソクロノスペイロード９５２の先頭のＣＩＰヘッダ９５４を除去した実データ９０５を復号化手段１２１に対して出力する。また、実データ抽出手段１２２は、ＣＩＰヘッダ９５４から抽出したソースＩＤ９０６と暗号化情報９１０とを鍵生成手段１２５に対して出力する。また暗号化情報９１０は、復号化手段１２１に対しても同様に出力される。鍵生成手段１２５は、送信装置１１０との間のエイシンクロナス通信のやり取りにより暗号鍵１２６を受け取り、復号化手段１２１に対して出力する。復号化手段１２１は、実データ抽出手段１２２から受信した暗号化情報９１０の値が０である場合には実データ抽出手段１２２から受け取った実データ９０５を映像音声化手段１２０に対してそのまま出力し、値が１である時には鍵生成手段１２５から受け取った暗号鍵１２６を用いて実データ９０５を復号化し、復号化した結果を映像音声化手段１２０に対して出力する。

【００２３】

図３は、本実施の形態における鍵生成手段１０６と鍵生成手段１２５との間でやり取りされるＡＫＥコマンド(AKE: Authentication and Key Exchange)のコマンドフォーマットおよびレスポンスフォーマットをあらわす図である。これらのコマンドおよびレスポンスは、ＡＶ／Ｃコマンドセットに属するコマンドとして、エイシンクロナス通信を用いて送信装置１１０と受信装置１２８との間でやり取りされる。これらのコマンドおよびレスポンスをやり取りすることにより、送信装置１１０および受信装置１２８の間で相手装置の認証や暗号鍵１０９，１２６のやり取りに必要な情報の交換を行う。ＡＫＥコマンドには、相手装置に対す

る何らかの動作を要求するＡＫＥコントロールコマンドと、相手装置の状態や能力を問い合わせるためのＡＫＥステイタスコマンドとがある。

【００２４】

図３（ａ）は、ＡＫＥステイタスコマンドのフォーマットをあらわす図である。ＡＫＥステイタスコマンドにおいて、オペコード２０８は、当該コマンドがＡＫＥコマンドであることを示す。アルゴリズムＩＤ２００は固定値０であり、０以外の値は将来の拡張のために予約となっている。

【００２５】

図３（ｂ）は、ＡＫＥステイタスコマンドに対するレスポンスのフォーマットをあらわす。図３（ａ）のＡＫＥステイタスコマンドを受け取った装置が、ＡＫＥステイタスコマンドの発行元の装置に対して返送するのがこのレスポンスである。送信装置１１０と受信装置１２８との間で相互認証および暗号鍵１０９，１２６の伝達を行う一連の情報交換手順には複数の種類があり、アルゴリズム領域２０１は、当該レスポンスを返す装置が実行可能な情報交換手順の識別子がビットアサインされている。すなわち、受信装置１２８が、暗号化されたＴＳＰを検出してから暗号鍵１０９，１２６を受け取るまでの間に、送信装置１１０との間で複数のコマンドおよびレスポンスをやり取りする。このコマンドおよびレスポンスをやり取りする情報交換手順には複数の種類があり、当該レスポンスを返す装置はどの情報交換手順を実行可能であるかという情報がアルゴリズム領域２０１の各ビットによってあらわされている。アルゴリズム領域２０１のサイズは１６ビットであるので、最大１６種類の情報交換手順をあらわすことが可能である。最大データ長２０２は、ＡＫＥコマンドおよびそれに対するレスポンスをやり取りする際に、受信可能な最大データ長が何バイトであるかを示す。

【００２６】

図３（ｃ）は、ＡＫＥコントロールコマンドのフォーマットをあらわす。ＡＫＥコントロールコマンドにおけるアルゴリズム領域２０１は、アルゴリズムＩＤ２００の値が０である時には、実行中の情報交換手順をあらわす。アルゴリズム領域２０１の各ビットは、ＡＫＥコントロールコマンドおよびＡＫＥコントロールコマンドに対するレスポンスにおいては必ず１つのビットだけが１となってお

り、その１ビットが現在実行中の情報交換手順をあらわしている。ラベル２０２は、複数のＡＫＥコントロールコマンド間の対応を明確にするために用いられる。例えば、装置が他の装置に対してＡＫＥコントロールコマンドを送信したとして、そのＡＫＥコントロールコマンドを受信した装置は、受信したＡＫＥコントロールコマンドに呼応する別のＡＫＥコントロールコマンドを返送するという規定が、ある情報交換手順で定められているとする。この場合、両ＡＫＥコントロールコマンド間の呼応関係を明確にするために、返送するＡＫＥコントロールコマンドに挿入されるラベル２０２は最初に受信したＡＫＥコントロールコマンドに挿入されていたラベル２０２と同じ値を使用する。ステップ番号２０３は、情報交換手順の中でやり取りされる個々のＡＫＥコントロールコマンドに対して１から順に付けられるシリアル番号である。

【００２７】

また、サブファンクション２９９は（表１）に挙げる値をとる。

【００２８】

【表１】

サブファンクション	値
メイクレスポンス	00_{16}
ベリファイミー	01_{16}
クリエイトキーインフォ	10_{16}
リコンストラクトキー	11_{16}
エクスチェンジ	20_{16}

【００２９】

サブファンクション２９９の内容がメイクレスポンスである場合に、当該ＡＫＥコントロールコマンドは、コマンドを受信する装置に対する認証のチャレンジを意味する。このときデータ２０７には、相手の装置を認証するための乱数である認証チャレンジデータが含まれる。このコマンドを受信した装置は、サブファンクション２９９の内容がベリファイミーであるＡＫＥコントロールコマンドを返送する。この返送の際にデータ２０７に格納されるデータは、先程受信したデータ２０７に対してあらかじめ定められた演算を行った結果である認証レスポン

スデータである。この演算に使用される鍵情報は、あらかじめ正規に認定された機器にのみ付与されている鍵であるので、返送されてきた認証レスポンスデータを調べれば、演算を行った機器が正しく認定された機器であるか否かを認証することができる。

【００３０】

サブファンクション２９９の内容がクリエイトキーインフォである場合に当該ＡＫＥコントロールコマンドは、コマンドを受信する装置に対する暗号鍵１０９の要求を意味する。このＡＫＥコントロールコマンドを受け取った装置は、サブファンクション２９９の内容がリコンストラクトキーであるＡＫＥコントロールコマンドを返送する。この時、データ２０７には暗号化された暗号鍵１０９が格納されて返送される。

【００３１】

サブファンクション２９９の内容がエクスチェンジである場合に当該ＡＫＥコントロールコマンドは、コマンドを送信する機器と受信する機器との間の鍵情報の交換を意味する。この鍵情報はデータ２０７に格納されて転送され、機器間の間接認証や、機器共有鍵の作成のために使用される。

【００３２】

（表１）に挙げられている以外のサブファンクションの値は将来の拡張のための予約となっている。チャネル番号２０４は、送信装置１１０および受信装置１２８の間で通信を行うアイソクロノス通信のチャネルの番号を示す。このチャネル番号２０４は、サブファンクション２９９の内容がクリエイトキーインフォまたはリコンストラクトキーの時にのみ有効であり、それ以外の場合にこの値は１６進表記でＦＦとなる。ブロック番号２０５および総ブロック番号２０６は、ＡＫＥコントロールコマンドでやり取りすべきデータが一つのＡＫＥコマンドで伝送しきれない場合に当該データを分割して送信する際に使用する。すなわち、総ブロック番号２０６は当該データを幾つに分割したかをあらわし、ブロック番号２０５によって、データ２０７が分割されたうちの幾つ目のデータであるかを示す。データ長２０９はデータ２０７に含まれる有効なデータのサイズをバイト数で表す。データ２０７はＡＫＥコントロールコマンドによってやり取りされるデ

ータである。ＡＫＥコントロールコマンドを受信した装置はＡＫＥコントロールコマンドに対する応答を返す。その際の応答のフォーマットおよび値は受け取ったＡＫＥコントロールコマンドのフォーマットおよび値と同じであるが、応答にはデータ２０７が含まれない点だけが唯一異なる。

【００３３】

図４は、送信装置１１０から受信装置１２８に対して暗号鍵１０９，１２６が送信されるまでの間に両装置間でやり取りされるＡＶ／Ｃコマンドの具体例を時間軸に沿って模式的にあらわした図である。まず、図４のＡＶ／Ｃコマンドのやり取りが始まるまでの両装置の動作を簡単に説明する。

【００３４】

まず初期状態として、暗号化されていないＴＳＰが送信装置１１０から送信されている状況を想定する。この時受信装置１２８は受信を行っていないものとする。信号源１００から出力されるＴＳＰが暗号化手段１０１に入力され、暗号化手段１０１は出力命令１０５の内容が通常出力であるのでＴＳＰを暗号化せずにそのままソースパケット化手段１０２に対して出力するとともに、暗号化情報９１０には値０を送信する。ソースパケット化手段１０２は受け取ったＴＳＰに４バイトのソースパケットヘッダを付加してＣＩＰブロック化手段１０３へと出力する。ＣＩＰブロック手段１０３はこれに８バイトのＣＩＰヘッダ９５４を付加し、アイソクロノスパケット化手段１０７に対してアイソクロノスペイロード９５２として出力する。この際、ＣＩＰヘッダ９５４に含まれる暗号化情報９１０は、暗号化手段１０１から入力した値である０をそのまま格納する。アイソクロノスパケット化手段１０７は入力したアイソクロノスペイロード９５２にアイソクロノスパケットヘッダ９００、ヘッダＣＲＣ９０１およびデータＣＲＣ９０３を付加してアイソクロノスパケットとして１３９４バス１１１上へと出力する。この際、アイソクロノスパケットヘッダ９００に含まれるタグ９０７の値は、当該アイソクロノスパケットがＡＶプロトコル準拠のアイソクロノスパケットであるので、１となる。

【００３５】

信号源１００から出力されるＴＳＰが変化した時、すなわち著作権で保護され

ていない映像音声情報から著作権で保護されている映像音声情報へと切り替わった時、この変化を検出した鍵生成手段１０６は出力命令１０５を通常出力から空出力へと変化させるとともに、ＴＳＰを暗号化するための暗号鍵１０９を暗号化手段１０１に渡す。

【００３６】

出力命令１０５の内容が空出力であるとき暗号化手段１０１は、信号源１００からＴＳＰを受け取るたびにソースパケット化手段１０２に対して空信号を出力するとともに暗号化情報９１０には値１が出力される。暗号化手段１０１から空信号を受け取ったソースパケット化手段１０２は、ソースパケットヘッダを付加せずに、受け取った空信号をそのままＣＩＰブロック化手段１０３へと伝達する。ＣＩＰブロック化手段１０３は空信号を受け取ると、ＣＩＰヘッダ９５４だけをアイソクロノスパケット化手段１０７へと出力する。この時、ＣＩＰヘッダ９５４中の暗号化情報９１０は、暗号化手段１０１から受信した値をそのまま用いる。アイソクロノスパケット化手段１０７はＣＩＰブロック化手段１０３から受け取ったＣＩＰヘッダ９５４をアイソクロノスペイロード９５２としてアイソクロノスパケットを作成し、１３９４パケット入出力手段１０８へ出力する。この際、当該アイソクロノスパケットはＡＶプロトコルに準拠しているので、タグ９０７の値は１となる。１３９４パケット入出力手段１０８は受け取ったアイソクロノスパケットを１３９４バス１１１上へと出力する。当該アイソクロノスパケットは継続的に出力され、１３９４バス１１１上にはＣＩＰヘッダ９５４のみをアイソクロノスペイロード９５２に含んだアイソクロノスパケットが継続的に流れるようになる。このアイソクロノスパケットを検出した受信装置１２８では、１３９４パケット入出力手段１２７がタグ９０７を調べ、ＡＶプロトコルに準拠したアイソクロノスパケットであることを検出した後当該アイソクロノスパケットをペイロード抽出手段１２３へと出力する。ペイロード抽出手段１２３は受け取ったアイソクロノスパケットからアイソクロノスペイロード９５２を抽出して実データ抽出手段１２２へと出力する。実データ抽出手段１２２ではＣＩＰヘッダ９５４に含まれる暗号化情報９１０とソースＩＤ９０６とを鍵生成手段１２５へと出力する。鍵生成手段１２５では、暗号化情報９１０を調べて値が１である

ことを検出したのち、ソースＩＤ９０６から当該アイソクロノスパケットを出力しているのが送信装置１１０であることを知る。しかる後鍵生成手段１２５はＡＶ／Ｃコマンドを用いて暗号鍵１０９，１２６を要求する過程、すなわち図４に示した過程へと移る。

【００３７】

図４において、ＡＫＥステイタスコマンド３００は受信装置１２８から送信装置１１０へと送信される。これにより受信装置１２８は、送信装置１１０が実行可能な情報交換手順を問い合わせることになる。これに応えて送信装置１１０はＡＫＥレスポンス３０１を受信装置１２８に対して返送する。このＡＫＥレスポンス３０１には送信装置１１０が実行可能な情報交換手順がアルゴリズム領域２０１内にビットアサインされており、受信装置１２８は送信装置１１０がどの情報交換手順を実行可能なのかを知ることができる。具体例としては、送信装置１１０が実行可能な情報交換手順が第２番目のものと第６番目のものの２つであった場合には、ＡＫＥレスポンス３０１内のアルゴリズム領域２０１は２進表記で「0000000000100010」となる。

【００３８】

ＡＫＥレスポンス３０１を受信した受信装置１２８は、送信装置１１０が実行可能でかつ受信装置１２８自身も実行可能な情報交換手順の中から最適な１つの手順を選択し、以降その手順にしたがってＡＶ／Ｃコマンドをやり取りする。いま仮に受信装置１２８の側で実行可能な情報交換手順が第２番目のものと第８番目のものであった場合には、送信装置１１０および受信装置１２８の双方で実行可能な情報交換手順は第２番目のものだけということになり、以降は第２番目の手順を用いて認証および情報の交換が行われることになる。この手順に含まれるＡＫＥコントロールコマンドでは、アルゴリズムＩＤの値が０で、アルゴリズム領域２０１の値が２進表記で「0000000000000010」となる。情報交換手順で指定される手順には、各種ＡＫＥコントロールコマンドのやり取りの順番だけでなく、各ＡＫＥコントロールコマンドで送られるデータ２０７のフォーマットや処理方法も規定されている。

【００３９】

第２番目の情報交換手順に従い、鍵生成手段１２５はメイクレスポンスコマンド３０２を送信装置１１０に対して送信する。このメイクレスポンスコマンド３０２の中のデータ２０７には、鍵生成手段１２５で発生させた２つの乱数ＲＲａとＲＲｂとが暗号化されて含まれているとともに、アルゴリズム領域２０１には第２番目の手順をあらわす識別情報が含まれている。この暗号化に際して使用する鍵は、あらかじめ正規に認められた送信装置と受信装置とに与えられている共通の秘密鍵である。メイクレスポンスコマンド３０２を受け取った鍵生成手段１０６は、受け取ったメイクレスポンスコマンド３０２のアルゴリズム領域２０１を調べて、以降は第２番目の手順を用いて認証および情報の交換を行うことを知る。鍵生成手段１０６は第２番目の手順を実行可能なのであるから、第２番目の手順に基づいて送信されてくるメイクレスポンスコマンド３０２のデータ２０７には秘密鍵で暗号化された２つの乱数が含まれていることを知っている。そこで鍵生成手段１０６は秘密鍵を用いてデータ２０７からＲＲａおよびＲＲｂの２つの乱数を取り出したのち、レスポンスを作成することが可能であることを示す応答３０３を返す。しかるのち鍵生成手段１０６は、取り出した乱数のうちの一つであるＲＲａをデータ２０７に格納してベリファイミーコマンド３０４を受信装置１２８に対して送信する。これが先程のメイクレスポンスコマンド３０２にて要求されたレスポンスである。このベリファイミーコマンド３０４を含め、以降、送信装置１１０と受信装置１２８との間でやり取りされるＡＫＥコマンドのアルゴリズム領域２０１には全て、２番目の手順をあらわす識別情報が含まれる。

【００４０】

ベリファイミーコマンド３０４を受信した鍵生成手段１２５は、データ２０７の内容であるＲＲａが、自分が先程発生させた乱数ＲＲａと相違無いことを確かめたのち、ベリファイミーコマンド３０４に対して正常にベリファイしたことを示す応答３０５を返す。これにより、鍵生成手段１２５は、送信装置１１０が正規に認められた送信装置であると認証する。

【００４１】

次に送信装置１１０が、先程と同じメイクレスポンスコマンド３０６およびベリファイミーコマンド３０８を用いて、受信装置１２８が正規に認められた受信

装置であることを確認する。この際に使用される乱数はＲＴａおよびＲＴｂであり、ベリファイミーコマンド３０８で送り返される乱数はＲＴｂである。

【００４２】

この時点で送信装置１１０および受信装置１２８の双方には、乱数ＲＲｂと乱数ＲＴｂとがともにわかっていることになる。また、お互いが正規に認められた装置であることを確認したことになる。鍵生成手段１０６と鍵生成手段１２５とは、それぞれ別個に、２番目の手順で定められている共通の演算方法により、ＲＲｂとＲＴｂとから一時鍵（図示せず）を生成する。この一時鍵は、送信装置１１０および受信装置１２８の両装置のみが共有する共通の鍵である。

【００４３】

次に鍵生成手段１２５はクリエイトキーインフォコマンド３１０を送信装置１１０に対して送信する。この際、クリエイトキーインフォコマンド３１０のチャネル番号２０４には、現在受信装置１２８が受信中のアイソクロノスパケットのチャネル番号が格納される。このクリエイトキーインフォコマンド３１０を受け取った鍵生成手段１０６は、ＴＳＰの暗号化に用いる暗号鍵１０９を一時鍵で暗号化したのち、クリエイトキーインフォコマンド３１０が正常に完了したことを示す応答３１１を返送する。鍵生成手段１０６はＴＳＰの暗号化に用いる暗号鍵１０９を一時鍵で暗号化した結果をデータ２０７に格納して、リコンストラクトキーコマンド３１２を用いて受信装置１２８へと送る。鍵生成手段１２５では一時鍵を用いてリコンストラクトキーコマンド３１２のデータ２０７を復号化し、その結果暗号鍵１２６を得たのち、リコンストラクトキーコマンド３１２を正常に完了したことをあらわす応答３１３を返す。暗号鍵１０９と暗号鍵１２６とは、同じ一時鍵を用いて暗号化と復号化を行ったので、同じ鍵である。暗号鍵１２６は鍵生成手段１２５から復号化手段１２１に対して出力される。

【００４４】

リコンストラクトキーコマンド３１２を送信した鍵生成手段１０６は、暗号化手段１０１に対して暗号化出力を示す出力命令１０５を出力する。これを受けた暗号化手段１０１は、信号源１００から受け取るＴＳＰを暗号鍵１０９で暗号化し、ソースパケット化手段１０２への出力を開始する。これにより、１３９４バス１１１上を、暗号鍵１０９にて暗号化されたＴＳＰをアイソクロノスペイロード９５２に含むアイソクロノスパケットが流れるようになる。当該アイソクロノスパケットは前述したように、復号化手段１２１において暗号鍵１２６を用いて復号化され、映像音声化手段１２０へと出力される。

【００４５】

上記一連のＡＫＥコントロールコマンドにおいて、メイクレスポンスコマンド３０２とベリファイミーコマンド３０４，メイクレスポンスコマンド３０６とベリファイミーコマンド３０８，クリエイトキーインフォコマンド３１０とリコンストラクトキーコマンド３１２はそれぞれ同じラベル２０２を持つ。また、メイクレスポンスコマンド３０２，ベリファイミーコマンド３０４，メイクレスポンスコマンド３０６，ベリファイミーコマンド３０８，クリエイトキーインフォコマンド３１０およびリコンストラクトキーコマンド３１２はそれぞれ１，２，３，４，５，６なる値をステップ番号２０３に持つ。

【００４６】

送信装置１１０の出力するアイソクロノスパケットに含まれる実データ部１０５が、暗号化された実データ１０５から暗号化されない実データ１０５へと変化した場合には、復号化手段１２１は暗号化情報９１０の変化を検出して復号化をやめ、実データ抽出手段１２２から受け取った出力をそのまま映像音声化手段１２０へと渡すようになる。

【００４７】

また、上記の図４に示した過程が始まった後に１３９４バス１１１にバスリセットが発生した場合には、メイクレスポンスコマンド３０２以降の手順を最初からやりなおす。

【００４８】

以上のように本実施の形態によれば、アイソクロノスパケット内の実データの

暗号化状況を示す暗号化情報が実データと一緒に送信されてデータ転送が行われることにより、アイソクロノスパケットを受信した受信装置がアイソクロノスパケット内に含まれる暗号化情報を調べ、実データが暗号化されていることを検出すると送信装置に対して実データを復号するための暗号鍵を要求し、要求を受けた送信装置は受信装置に対して暗号鍵を付与するので、送信装置が受信装置に復号のための暗号鍵を付与する際の手順が極めて簡素なデータ転送方法を実現できる。

【００４９】

また、アイソクロノス通信で転送されるアイソクロノスパケットには実データの暗号化状況を示す暗号化情報と実データとが含まれ、暗号化は実データに対してのみ行ってデータ転送を行うことにより、従来のデータ転送方法との互換性を保ちつつ、かつ従来の受信装置が暗号化された実データを受信しても誤動作する可能性のないデータ転送方法を実現できる。

【００５０】

さらに、送信装置の送信している同期データを受信装置が継続的に受信している最中に同期データの暗号化が始まったとしても、ＣＩＰヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できる。

【００５１】

なお、本実施の形態においては、暗号鍵による暗号化が一旦開始すれば全ての転送単位に含まれる実データは暗号化されて送信されるが、全ての転送単位に対して暗号化を行う必要はない。例えば、暗号化された転送単位と暗号化されない転送単位とが交互に送信されても、ＣＩＰヘッダ中に暗号化情報が含まれているので受信装置においては復号を正常に行うことが可能であり、同様の効果を得ることが可能である。この場合、暗号化を行う転送単位の割合を受信装置が送信装置に指定しても得られる効果が変わらないことは言うまでもない。また、ＭＰＥＧのソースパケットはその大きさが１９２バイトであるが、ＭＥＰＧの高データレート転送（１２Ｍｂｐｓ以上）を行う際には複数のソースパケットが一つのアイソクロノスペイロードに格納される。このとき、同一のアイソクロノスペイロ

ードの中に、暗号化されたソースパケットと暗号化されないソースパケットとの両方があってはならないことも言うまでもない。

【００５２】

また、本実施の形態においては、暗号鍵による暗号化は実データ部全てに対して行われたが、全ての部分に暗号化を行う必要はない。例えば実データ部の前半分だけを暗号化したり、実データ部を４等分したうちの最初と３番目の２個所を暗号化して送信しても同様の効果が得られる。この場合は暗号化を行った場所や割合を示す情報をＣＩＰヘッダに挿入して送信すれば受信装置側で適切な復号化を行うことが可能である。また、ＣＩＰヘッダには実データが暗号化されているか否かを示す暗号化情報のみを挿入しておき、ＣＩＰヘッダを見て暗号化されていることを検出した受信装置が、どの部分がどのくらい暗号化されているかという情報をエイシンクロナス通信を用いて送信装置に問い合わせても同様の効果を得ることが可能である。この場合、暗号化を行う場所や割合を受信装置の側が送信装置に対してエイシンクロナス通信を用いて指定しても同様の効果が得られることは言うまでもない。また、実データ部の中でデータの重要性が高い部分についてのみ暗号化を行うと、暗号化および復号化にかかる負荷が低いにもかかわらず十分な暗号化の効果が得られることも言うまでもない。

【００５３】

また、本実施の形態においては、送信装置と受信装置との間の相互の認証が完了するまでの間は実データを含まないＣＩＰヘッダのみのアイソクロノスパケットを転送したが、ＣＩＰヘッダのみのアイソクロノスパケットを出力することなく最初から暗号化された実データを含むアイソクロノスパケットを出力しても同様の効果が得られることは言うまでもない。

【００５４】

また、本実施の形態においては、送信装置と受信装置の間でやり取りされるＡＫＥコントロールコマンドの転送手順を相互の調停により決定したが、受信装置が実行可能な手順が一つだけに限られる場合にはこの調停手順を行わず、受信装置が実行可能な唯一の手順でコマンドの転送を開始しても同様の効果が得られることは言うまでもない。こういった場合には、全ての正規に認証された機器が最

低限実行可能な基本手順を定めておくことが望ましい。

【００５５】

また、本実施の形態においては、送信装置と受信装置との間で直接認証を行い、秘密鍵による復号化情報の伝送を行ったが、認証および復号化情報の伝達手段はこれに限らない。例えば公開鍵を用いて相互に間接認証および一時鍵の作成を行い、一時鍵を用いて復号化情報の伝送を行っても構わない。以下、その手順を簡単に説明する。

【００５６】

送信装置および受信装置は、相互の調停の結果定められた手順により、相互の間接認証に必要となる鍵情報をＡＫＥコントロールコマンドのデータ２０７に格納して送信しあう。このとき、サブファンクション２９９はエクスチェンジをあらわす。これにより、送信装置と受信装置は互いに正規に認証された機器であれば同じ一時鍵を共有することになるので、それ以降は本実施の形態と同様にクリエイトキーインフォコマンドおよびリコンストラクトキーコマンドを用いて復号化情報の伝送を行うことが可能となる。

【００５７】

【発明の効果】

以上のように本発明のデータ転送方法では、同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データ部と一緒に送信されてデータ転送が行われることにより、同期データを受信した受信装置が同期データ内に含まれる暗号識別情報を調べ、実データ部が暗号化されていることを検出すると送信装置に対して実データ部を復号するための復号化情報を要求し、要求を受けた送信装置は受信装置に対して復号化情報を付与するので、送信装置が受信装置に復号のための鍵情報を付与する際の手順が極めて簡素なデータ転送方法を実現できるという優れた効果がある。

【００５８】

また、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行ってデータ転送を行うことにより、従来のデータ転送方法との互換性を保ちつつ、かつ

従来の受信装置が暗号化された同期データを受信しても誤動作する可能性の無いデータ転送方法を実現できるという優れた効果がある。

【００５９】

また、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行ってデータ転送を行うことにより、送信装置の送信している同期データを受信装置が継続的に受信している最中に同期データの暗号化が始まったとしても、ＣＩＰヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できるという優れた効果がある。

【００６０】

また、送信装置と受信装置の間でやり取りされる認証情報および復号化情報の授受手順を送信装置と受信装置との間の調停によって選択することにより、将来の拡張性に優れた認証および復号化情報の授受手順を実現することが可能となる。すなわち、将来新しい認証方法や復号化情報が利用可能になった際に、新しい手順を使用できる機器と古い手順しか使用できない機器とが混在しても、新しい機器側で古い手順を使用可能であれば、両機器間の調停により最適な手順を選択することが可能になる。すなわち本発明のデータ転送方法では、新しい機器と古い機器とが混在する環境においても、常に最適な手順を選択して実行可能になるという優れた効果がある。

【００６１】

また、暗号化された実データと暗号化されない実データとの割合を変化させることが可能であるので、暗号化された実データを復号するための特別なハードウェアを持たない受信装置でもソフトウェアによって復号化が可能になる。すなわち、パソコンのように特別な復号のためのハードウェアを持たない機器が受信装置である場合にも、暗号化される実データの割合を低下させることによりソフトウェアによる復号が可能になるという優れた効果がある。

【００６２】

また、実データの中で暗号化する部分や割合を変化させることが可能であるので、暗号化された実データを復号するための特別なハードウェアを持たない受信

装置でもソフトウェアによって復号化が可能になる。すなわち、パソコンのように特別な復号のためのハードウェアを持たない機器が受信装置である場合にも、実データの中で暗号化する部分の割合を低下させることによりソフトウェアによる復号が可能になるという優れた効果がある。

【００６３】

また、送信装置と受信装置が相互に正規の機器であることを認証するまでの間は実データを含まないアイソクロノスパケットを出力するので、限られたバスの転送帯域を無駄に使用することがなく、また正規に認証されていない機器が実データを受信してしまう可能性が非常に少なくなるという優れた効果がある。

【図面の簡単な説明】

【図１】

本発明の実施の形態におけるＣＩＰヘッダのフォーマットを表す模式図

【図２】

同実施の形態における送信装置と受信装置との構成を示すブロック図

【図３】

（ａ）同実施の形態におけるＡＫＥステイタスコマンドのフォーマットを表す説明図

（ｂ）同実施の形態におけるＡＫＥステイタスコマンドに対するＡＫＥレスポンスのフォーマットを表す説明図

（ｃ）同実施の形態におけるＡＫＥコントロールコマンドのフォーマットを表す説明図

【図４】

同実施の形態による送信装置と受信装置との間のエイシンクロナスパケットの授受を表す模式図

【図５】

従来のデータ転送方法におけるアイソクロノスパケットのフォーマットを表す説明図

【符号の説明】

１０１　暗号化手段

１０２　ソースパケット化手段

１０３　ＣＩＰブロック化手段

１０６、１２５　鍵生成手段

１０７　アイソクロノスパケット化手段

１０８、１２７　１３９４パケット入出力手段

１１０　送信装置

１１１　ＩＥＥＥ１３９４バス

１２１　復号化手段

１２２　実データ抽出手段

１２３　ペイロード抽出手段

１２８　受信装置

９００　アイソクロノスパケットヘッダ

９０１　ヘッダＣＲＣ

９０２、９５２　アイソクロノスペイロード

９０３　データＣＲＣ

９０４、９５４　ＣＩＰヘッダ

９０５　実データ

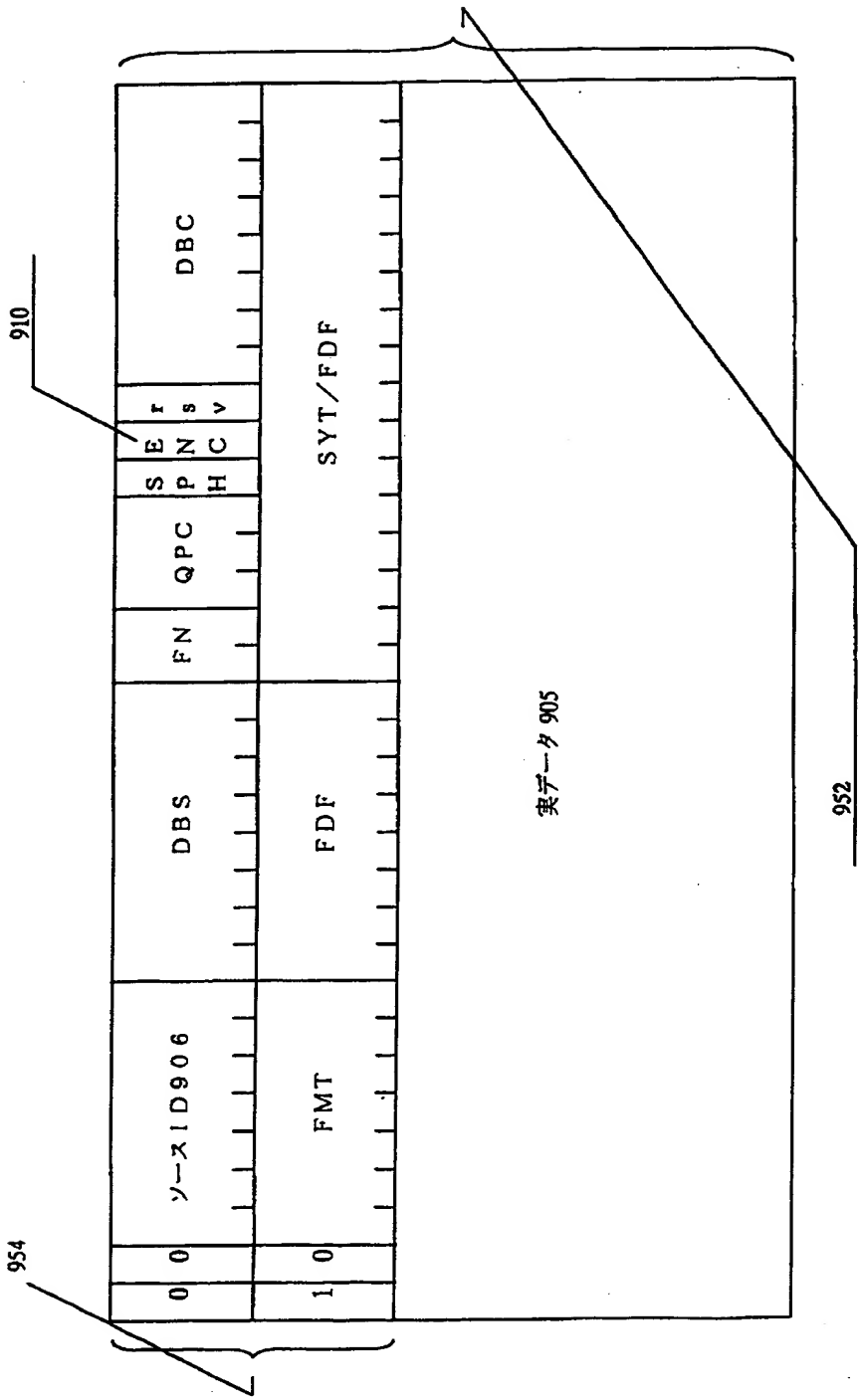
９０６　ソースＩＤ

９０７　タグ

９１０　暗号化情報

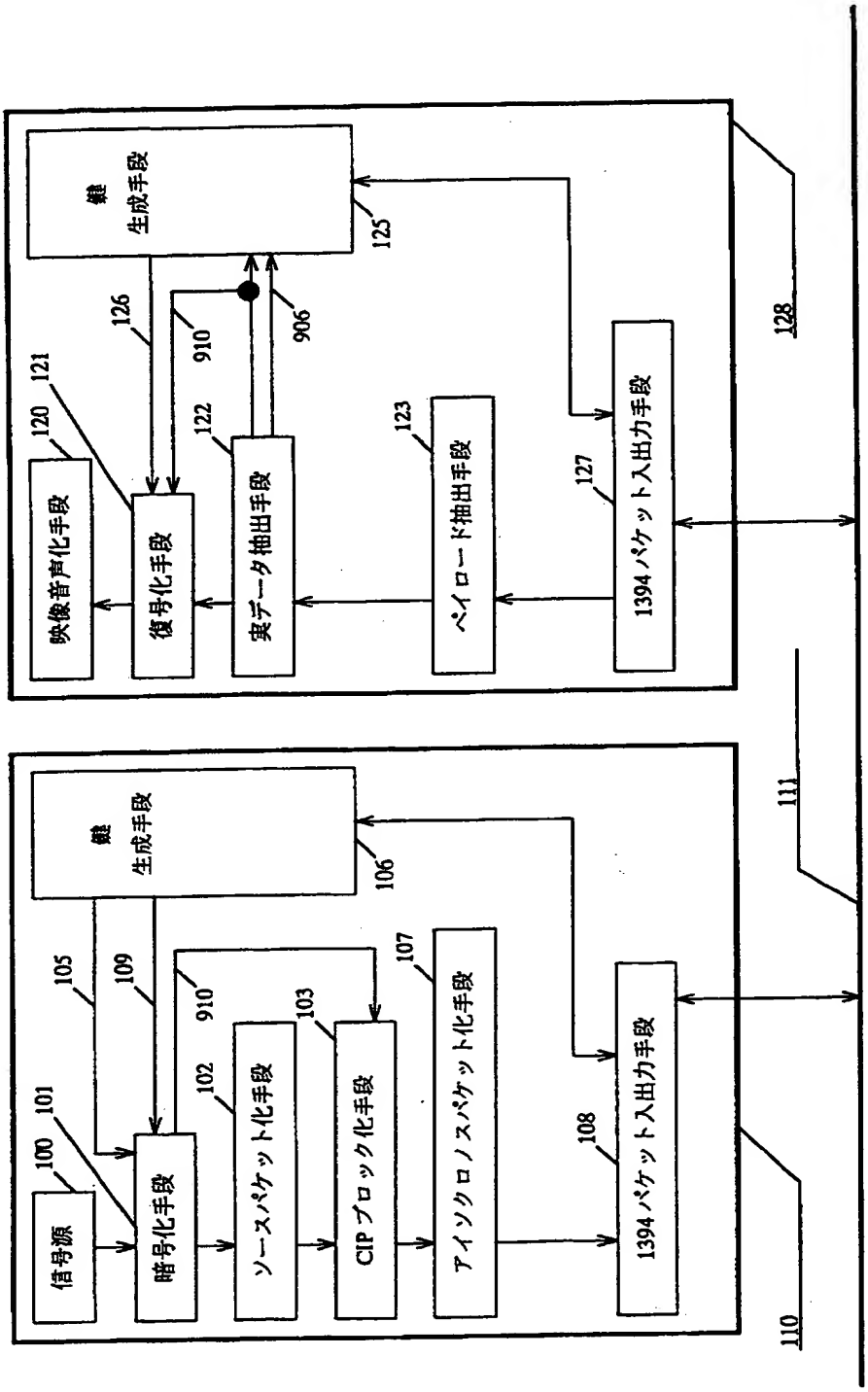
【書類名】　図面

【図１】



出証特平１０－３０４２５１２

【図2】


鍵
生成手段
125
126
910
906
121
120
122
123
127
128
映像音声化手段
復号化手段
実データ抽出手段
ペイロード抽出手段
1394パケット入出力手段
鍵
生成手段
106
111
105
109
910
107
103
102
101
100
108
信号源
暗号化手段
ソースパケット化手段
CIPブロック化手段
アイソクロノスパケット化手段
1394パケット入出力手段
110

【図３】

(a)

	msb ／ オペコード208	lsb
opcode	Authentication and Key exchange	
operand[0]	F_{16}	アルゴリズムＩＤ200
operand[1]	FF_{16}	
operand[2]	FF_{16}	
operand[3]	FF_{16}	
operand[4]	FF_{16}	
operand[5]	FF_{16}	
operand[6]	FF_{16}	
operand[7]	FF_{16}	
operand[8]	FF_{16}	

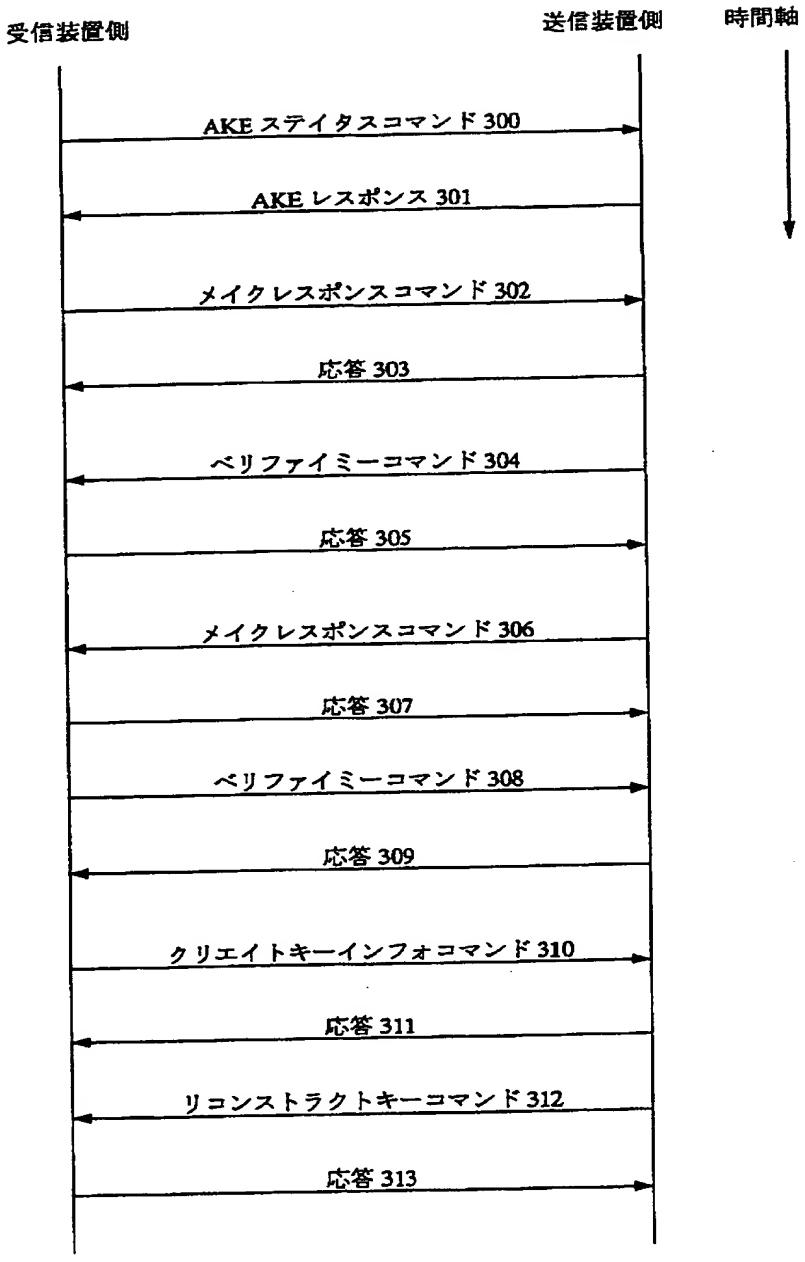
(b)

	msb ／ オペコード208	lsb
opcode	Authentication and Key exchange	
operand[0]	0	アルゴリズムＩＤ200
operand[1]	(msb) アルゴリズム領域201	
operand[2]		(lsb)
operand[3]	FF_{16}	
operand[4]	FF_{16}	
operand[5]	FF_{16}	
operand[6]	FF_{16}	
operand[7]	(msb) 最大データ長202	
operand[8]		(lsb)

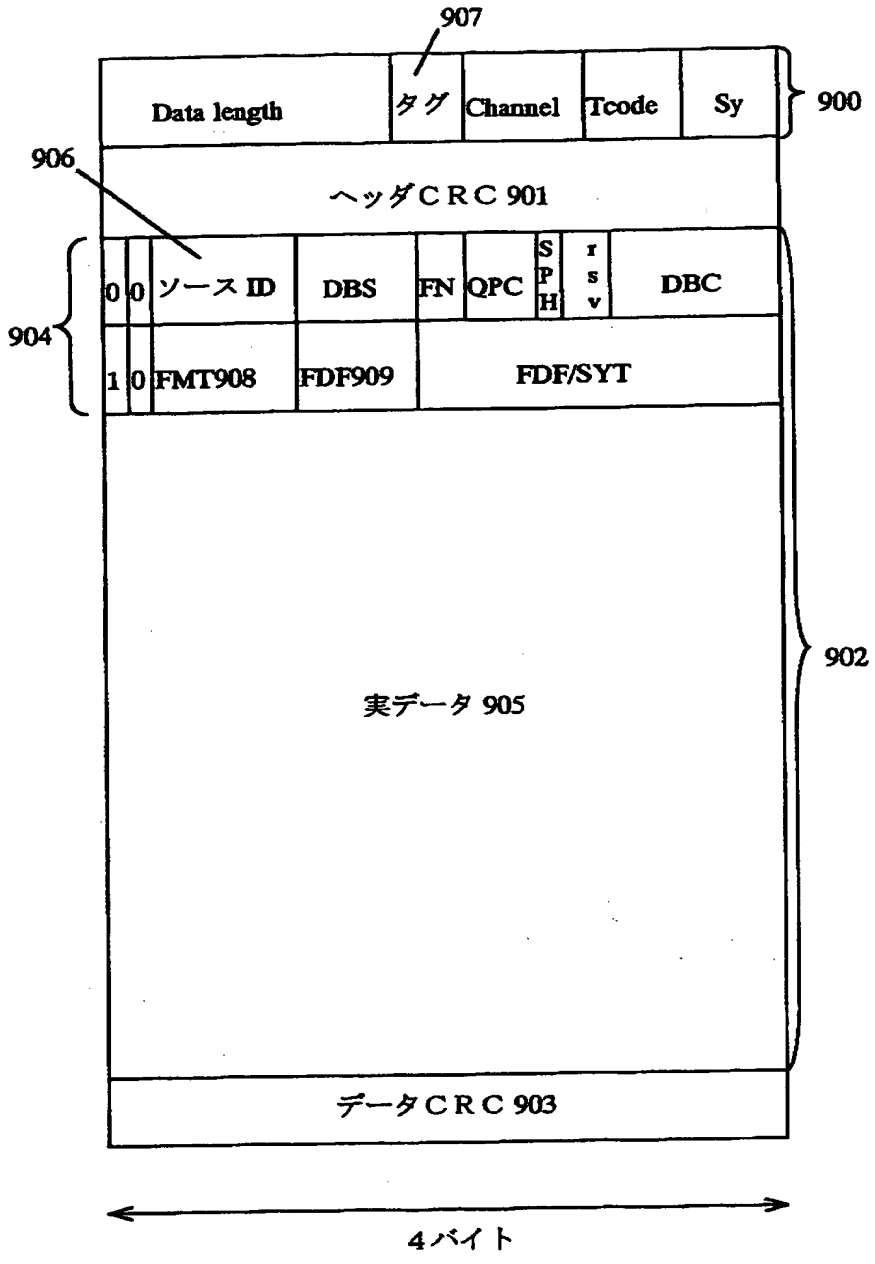
(c)

	msb ／ オペコード208	lsb
opcode	Authentication and Key exchange	
operand[0]	reserved	アルゴリズムＩＤ200
operand[1]	(msb) アルゴリズム領域201	
operand[2]		(lsb)
operand[3]	ラベル202	ステップ番号203
operand[4]	サブファンクション299	
operand[5]	チャネル番号204	
operand[6]	ブロック番号205	総ブロック番号206
operand[7]	(msb) データ長209	
operand[8]		(lsb)
operand[9]	データ207	
:		
operand[8+ data_length]		

【図４】


受信装置側
送信装置側
時間軸
AKE ステイタスコマンド 300
AKE レスポンス 301
メイクレスポンスコマンド 302
応答 303
ベリファイミーコマンド 304
応答 305
メイクレスポンスコマンド 306
応答 307
ベリファイミーコマンド 308
応答 309
クリエイトキーインフォコマンド 310
応答 311
リコンストラクトキーコマンド 312
応答 313

【図５】


907
Data length
タグ
Channel
Tcode
Sy
900
906
ヘッダＣＲＣ 901
0
0
ソース ID
DBS
FN
QPC
SPH
rsv
DBC
904
1
0
FMT908
FDF909
FDF/SYT
902
実データ 905
データＣＲＣ 903
4バイト

【書類名】　要約書

【要約】

【課題】　ＩＥＥＥ１３９４バスで、著作権により保護されたＡＶ情報を暗号化して送信する際に、暗号化に対応していない従来の機器も誤動作することのないデータ転送方法を提供することを目的とする。

【解決手段】　暗号化は実データ部９０５に対してのみ行い、ヘッダ９５４は暗号化せずに送信する。実データ部９０５が暗号化されているかどうかを示す暗号識別情報９１０がヘッダ９５４内に配置される。これにより、従来の規格を満足し、かつ従来の機器が暗号化されたパケットを受信しても誤作動することがない。

【選択図】　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005821
【住所又は居所】　大阪府門真市大字門真１００６番地
【氏名又は名称】　松下電器産業株式会社
【代理人】　申請人
【識別番号】　100078204
【住所又は居所】　大阪府門真市大字門真１００６　松下電器産業株式会社内
【氏名又は名称】　滝本　智之
【選任した代理人】
【識別番号】　100097445
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名又は名称】　岩橋　文雄

出　願　人　履　歴　情　報

識別番号　　〔000005821〕

1．変更年月日　　1990年　8月28日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真1006番地
氏　名　　松下電器産業株式会社